Remarks

Claims 1-29 are currently pending in the patent application. For the reasons and arguments set forth below, Applicant respectfully submits that the claimed invention is allowable over the cited references.

In the instant Office Action dated December 31, 2007, the following rejections are noted: claims 10, 12, 14-19 and 25-27 stand rejected under 35 U.S.C. § 102(a) over Hatonen (U.S. Patent Pub. 2004/0039968); claims 1-4, 11 and 20-23 stand rejected under 35 U.S.C. § 103(a) over Hatonen in view of Jalali (U.S. Patent No. 6,694,469); claim 24 stands rejected under 35 U.S.C. § 103(a) over Hatonen and Jalali in view of Earl (U.S. Patent Pub. 2003/0233594); and claims 5-9, 13, 28 and 29 stand rejected under 35 U.S.C. § 103(a) over Earl in view of Hatonen. Applicant respectfully traverses these rejections.

With regard to the § 102(a) rejection of claims 10, 12, 14-19 and 25-27 over Hatonen, Applicant submits that the cited portions of the Hatonen reference fail to correspond to various aspects recited in the claims, including receiving a report of a modification or corruption of an information file, determining validity of the report, or degrading the trustworthy-measure associated with the node supplying the information file when the report is determined to be valid. The cited portions of Hatonen discuss real-time troubleshooting of network problems, such as quality of service problems, by detecting anomalies in the behavior of observable objects such as network elements, subscribers, subscriber groups, geographical areas, circuit groups, services, and the like (*see, e.g.*, Hatonen paragraphs 0014-0019 and 0028-0029). The Hatonen reference appears to be unrelated to detecting modified or corrupted information files in a distributed network in the manner recited by Applicant's claims. In fact, Applicant finds nothing in the Hatonen reference to teach information file sharing over a distributed network, much less detecting and reporting whether information files received within a distributed network have been corrupted, determining the source node for such corrupted files, and adjusting the trustworthiness of the source nodes supplying the corrupted files (or alternatively and optionally adjusting the trustworthiness of the reporting node if the corruption report is determined to be invalid).

For at least these reasons, Applicant submits that the § 102(a) rejection is improper because the Hatonen reference fails to teach or suggest all the elements of claims 10, 12, 14-19 and 25-27. Reconsideration and withdrawal of the rejection are requested.

Applicant submits that the § 103(a) rejection of claims 1-4, 11 and 20-23 over Hatonen in view of Jalali is improper because the proposed combination fails to teach or suggest all the claim elements, and because no valid reason to make the proposed combination has been presented. It is admitted in the Office Action that Hatonen fails to teach computing a code based on the content of a received information file, the computed code being used to determine whether the information file has been modified or corrupted, for example by comparing the computed code to an identifying code of the information file that is based on the content of the information files when it was introduced into the network. Applicant submits that the cited portion of Jalali fails to cure these admitted deficiencies of Hatonen. Jalali appears to disclose receiving a communications packet at a terminal (such as a cellular phone), computing a quality metric for the packet (such as a cyclic redundancy check), and requesting retransmission of the packet if the computed quality metric does not match a quality metric contained in the packet. Applicant submits that there is nothing in Jalali to teach or suggest that the communications packet is an information file to be shared among nodes in a distributed network, or that the quality metric comparison has anything to do with file modification or corruption as provided by the source. Moreover, Applicant finds nothing in Jalali to cure the underlying deficiencies of the Hatonen reference as noted in the above discussions. In particular, neither Hatonen nor Jalali appear to be related to sharing information files in distributed networks where any node can be a source of the information files.

Applicant understands from Jalali that quality metric mismatches arise from imperfect packet transmissions and incorrect packet decoding, and result in requests for retransmission of the packet. Applicant submits that one of skill in the art would not use a quality check technique for determining whether to request retransmission of the same information from the same source as a way to detect corrupted files and report the source of the corrupted files for the purpose of degrading the trustworthiness of the source. As such, there is no valid reason to modify the teachings of Hatonen to include the quality check of

Jalali, and such modification would not result in the claimed corruption detection and controlling of source node trustworthiness.

For at least these reasons, Applicant submits that the § 103(a) rejection of claims 1-4, 11 and 20-23 is improper. Reconsideration and withdrawal of the rejection are requested.

With respect to the § 103(a) rejection of claim 24 over Hatonen and Jalali in view of Earl, Applicant submits that the rejection is improper at least due to the impropriety of the underlying combination of Hatonen and Jalali as applied to claims 20, 21 and 23 (from which claim 24 depends), as noted above. Moreover, Applicant understands that it is admitted in the Office Action that the proposed combination of Hatonen and Jalali fails to teach the claimed feature of making the trustworthy-measure of the source node available for access to the other nodes to facilitate control of further file distribution. In view of this deficiency, the Earl reference is sought to be combined with Hatonen and Jalali. Applicant submits, however, that the cited portions of Earl do not correspond to the features recited in Applicant's claims. Earl appears to teach monitoring the state of various components in a network (for example, which components are operative), and making the state information available throughout the network. Applicant finds nothing in Earl to teach or suggest that such component monitoring has anything to do with a trustworthy-measure of a source node determined to be unreliable, for example due to providing corrupted files. The teachings of Earl appear to be directed to detecting which components in a network are operating correctly and to distributing such state information across the network, as opposed to being directed to distributing a trustworthy-measure associated with file transfer from a particular node to facilitate control of subsequent file distribution decisions.

For at least these reasons, Applicant submits that the § 103(a) rejection of claim 24 is improper. Reconsideration and withdrawal of the rejection are requested.

Applicant submits that the § 103(a) rejection of claims 5-9, 13, 28 and 29 over Earl in view of Hatonen is improper because the proposed combination fails to teach or suggest all the claim elements. In view of the discussions above, Applicant submits that neither the Earl reference nor the Hatonen reference appear to disclose processing and verifying error reports based on the receipt of corrupted files from a node in a distributed network, degrading a trustworthy-measure of that node, and providing the trustworthy-measure to

another node in the network to facilitate control of further file distribution. For example, none of the cited portions of the Earl reference correspond to providing the trustworthy-measure of a source node to other nodes, where such trustworthy-measure has been degraded due to an error report based on receiving a corrupted file from the source node. Rather, Earl monitors for failed links and devices within a network and provides prompt delivery of failure notices. Applicant submits that the monitoring and delivery of failure notices disclosed by Earl is unrelated to detecting the distribution of corrupted files within a distributed network, determining the source node of such corrupt file distribution, degrading the trustworthiness of the source node, and facilitating control of further file distribution accordingly. Moreover, the Hatonen reference discloses detecting and reporting anomalous behavior of network elements based on certain performance criteria, and appears to be unrelated to reporting the distribution of corrupted files and degrading the trustworthiness of source nodes.

For at least these reasons, Applicant submits that the § 103(a) rejection of claims 5-9, 13, 28 and 29 is improper. Reconsideration and withdrawal of the rejection are requested.

Applicant further submits that the cited art does not appear to teach or suggest the features additionally recited in newly-added claims 30-34 in combination with the features recited in the claims from which they depend.

In view of the remarks above, Applicant believes that each of the rejections has been overcome and the application is in condition for allowance. Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the agent overseeing the application file, Peter Zawilski, of NXP Corporation at (408) 474-9063.

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131

CUSTOMER NO. 65913

By: _____
Name: Robert J. Crawford
Reg. No.: 32,122
(NXPS.448PA)